Australian Government
Department of Defence
Defence Science and
Technology Organisation

Don't Judge a (Face)Book by its Cover: A Critical Review of the Implications of Social Networking Sites

Kathryn Parsons, Agata McCormac and Marcus Butavicius

Command, Control, Communications and Intelligence Division
Defence Science and Technology Organisation

DSTO-TR-2549

ABSTRACT

Social networking sites (SNS) are increasingly popular, and as their popularity continues to grow, the integration of these sites within the workplace is vitally important. Although these sites may provide a number of advantages, such as improved knowledge sharing and improved relationships, there are also numerous risks associated with the use of these sites. For example, these sites may jeopardise privacy, security and confidentiality, may waste company time, and may create tension within the workplace. Hence, it is crucial for organisations to develop a clear and enforceable policy for the use of these sites, which should be coupled with a personal, meaningful and contextualised education campaign. It is vital to emphasise the possible risks, reinforce the restrictions to use, and stress the consequences of a failure to comply. This should help to ensure that organisations can benefit from the advantages of these sites, without unnecessarily jeopardising their security.

Published by

Command, Control, Communications and Intelligence Division
DSTO Defence Science and Technology Organisation
PO Box 1500
Edinburgh South Australia 5111 Australia

Telephone: (08) 7389 5555
Fax: (08) 7389 6567

AR-014-995
May 2011

APPROVED FOR PUBLIC RELEASE

Don't Judge a (Face)Book by its Cover: A Critical Review of the Implications of Social Networking Sites

Executive Summary

Social networking sites (SNS) are services that allow users to build online profiles to share information with each other. The use of these sites is rapidly growing, and the most popular sites now have in excess of 300 million members. Although these sites are currently most popular with teenagers and young adults, the fastest growing demographic is those aged 35 years and older.

Hence, the use of these sites within the workplace is likely to increase, and it is therefore vital to understand how these sites alter relationships and workplaces. It is increasingly important for organisations to have a clear understanding of the possible implications of these sites, and it is crucial for organisations to determine what restrictions on the use of these sites are necessary and reasonable.

Essentially, these sites can offer a number of advantages; they can assist with knowledge and information sharing, and can improve relationships and provide emotional support. However, there are also a number of potential disadvantages associated with the use of these sites. For example, these sites can waste company time, can disrupt the working environment, and can expose an organisation to numerous security vulnerabilities.

These threats are particularly serious, since evidence suggests that many users of SNS do not consider the security implications of their behaviour, and have an inadequate level of caution when utilising these sites. Hence, these users may jeopardise the security, privacy and confidentiality of their organisations.

It is therefore vital for organisations to determine whether the use of SNS will be forbidden, tolerated or encouraged, and they should then develop an associated policy. This policy should cover issues associated with defamation, confidentiality, privacy and misleading conduct, and it should be clear, and enforceable.

Furthermore, since many of the users of these sites lack an awareness or comprehension of the potential risks, it is also crucial to improve employee education. This should emphasise the possible risks, reinforce any necessary restrictions to use, and stress the consequences associated with a failure to comply. Evidence also suggests that education is most effective when it is personal, meaningful and contextualised, and therefore case studies can greatly enhance the effectiveness of an education campaign.

This page is intentionally blank

Authors

Kathryn Parsons
Command, Control, Communications and Intelligence

Kathryn Parsons is a research scientist with the Human Interaction Capability Discipline in C3ID where her work focuses on cognitive and perceptual psychology, information visualisation and interface design. She obtained a Graduate Industry Linked Entrepreneurial Scheme (GILES) Scholarship in 2005, with Land Operations Division, where she was involved in human factors research, in the Human Sciences Discipline, specifically in the area of Infantry Situation Awareness. She completed a Master of Psychology (Organisational and Human Factors) at the University of Adelaide in 2005.

Agata McCormac
Command, Control, Communications and Intelligence

Agata McCormac joined DSTO in 2006. She is a research scientist with the Human Interaction Capability Discipline in C3ID where her work focuses on cognitive and perceptual psychology, information visualisation and interface design. She was awarded a Master of Psychology (Organisational and Human Factors) at the University of Adelaide in 2005.

Marcus Butavicius
Command, Control, Communications and Intelligence

Marcus Butavicius is a research scientist with the Human Interaction Capability Discipline in C3ID. He joined LOD in 2001 where he investigated the role of simulation in training, theories of human reasoning and the analysis of biometric technologies. In 2002, he completed a PhD in Psychology at the University of Adelaide on mechanisms of visual object recognition. In 2003 he joined ISRD where his work focused on data visualisation, decision-making and interface design. He is also a Visiting Research Fellow in the Psychology Department at the University of Adelaide.

This page is intentionally blank

Contents

This page is intentionally blank

1. Introduction

The use of social networking sites (SNS), both within and outside of organisations, is extremely common and is growing at a rapid rate. This growth not only includes students and young adults, who are "a generation whose identity has been forged online" (Rosenblum, 2007, p40), but also includes older generations. Recent reports indicate that the fastest growing demographic on SNS is those 35 years and older (Facebook, 2009a). Hence, the integration of these sites within the workplace is increasingly important. It is vital to understand how these sites alter relationships, and impact upon the workplace dynamic (DiMicco, Millen, Geyer & Dugan, 2008).

It is also important for organisations to have a clear understanding of what restrictions on the use of these sites are necessary and reasonable. For example, can or should an organisation limit an employee's interaction with SNS when off-duty? It seems clear that restrictions are necessary in regard to work related information (e.g., it is clearly inappropriate to post any proprietary company knowledge in a public forum). However, would it also be reasonable for an organisation to place limits on non-work related information? The manner in which employees are represented online may reflect poorly on the professionalism of the organisation, and therefore, in some cases, it could be reasonable (or even essential) to place limits on non-work related postings. Furthermore, the use of SNS may result in security vulnerabilities. Therefore, although there are potential advantages associated with SNS, it is also vital to determine whether these advantages outweigh the risks.

Essentially, it is extremely important for an organisation to have a clear policy regarding the use of these sites. Organisations may choose to ban them, but this may be an impracticable and limiting decision, and it is possible that severe restrictions may not be adhered to. For example, in 2004, Microsoft released a directive that using sites such as LinkedIn was a violation of company policy (Skeels & Grudin, 2009). Four years later, approximately 30% of employees (including executive level employees) were using the site (Skeels & Grudin, 2009). Perhaps rather than banning these sites, it would be more constructive to provide employees with the information required to make smart decisions (e.g., what information should be shared in what contexts). This would encourage employees to exercise judgement regarding whether personal information should be publicly available (Rosenblum, 2007). It is also crucial to inform people that complacency regarding the dissemination of information can have dangerous or embarrassing results (Rosenblum, 2007).

This report will provide a review of the current literature in the use of SNS, with a particular focus on use within the workplace. It will examine both the possible advantages associated with the use of these sites, and the potential dangers and vulnerabilities. The distinction between general SNS sites, which are open to the public, and enterprise SNS, which are internal to an organisation, will also be explained. A number of recommendations will also be provided.

2. An Overview of Social Networking Sites

Reports regarding the frequency and popularity of SNS are constantly changing. The most popular sites currently have hundreds of millions of users, and that number is rapidly increasing. For example, according to Nielson (2009), Facebook had a 700% increase in users from April 2008 to April 2009.

There are a vast number of different sites, and although they vary greatly in their purpose and functionality, they generally have certain features in common. The majority of sites include a profile page, where users can provide personal information, such as age, location and interests. Most sites also allow an individual to maintain a list of other users with whom they share a connection (Boyd & Ellison, 2007), and these sites usually have privacy controls to limit which aspects of this information can be viewed by which people.

Many of these various sites focus on a particular domain or interest area (e.g., travel, photos, music or books), and some sites have restrictions to their use. This may include limits to a particular age group, or could include only people who have received an invitation. Sites also vary greatly in the manner in which these details are verified; the majority of sites have little or no verification, and instead, trust that the information provided by users is authentic.

The content on SNS also varies greatly. Some sites focus primarily on the social networking aspect, whilst others are more focused on the blogging aspect. Many sites also include a micro-blogging component, where users can provide a short update (usually a maximum of 150 characters) to seek or share information. This could include details of their daily lives, or opinions and news (Java, Song, Finin & Tseng, 2007; McFedries, 2007).

The manner in which these sites are utilised also varies. Lampe, Ellison and Steinfield (2006) categorise these uses as 'social browsing' or 'social searching'. Social browsing involves using SNS to develop new contacts, and social searching refers to finding more about current offline contacts. Furthermore, some organisations now encourage employees to use SNS to interact with fellow employees and clients, and to disseminate and acquire information (Skeels & Grudin, 2009).

Recent reports indicate that SNS are used frequently in the workplace; in a survey of over 500 employees, 51% admitted to visiting these sites at least once per day (FaceTime, 2008). In this report, 79% of respondents indicated that they use SNS at work for business reasons, and 82% indicated that they use them for personal reasons (FaceTime, 2008). However, according to Wang and Kobsa (2009), SNS usage in the workplace is predominantly for social purposes rather than business purposes.

Wang and Kobsa (2009) also distinguish between general SNS, which are open to the public for registration, and enterprise SNS, which are internal to a particular company or organisation and are only available to its employees. An increasing number of organisations are implementing these enterprise SNS. More information regarding these types, including details of some of the most popular sites, will now be provided.

2.1 General Social Networking Sites

The most commonly used general SNS sites include Facebook[1], Twitter[2], LinkedIn[3], MySpace[4] and YouTube[5]. However, as mentioned previously, this is a very dynamic area and the popularity of sites changes very quickly.

At the time of writing, Facebook is the most popular SNS, and is ranked second in Alexa's (2009) Australian traffic ranking[6], which is a measure of a website's popularity. In October 2009, it was reported that Facebook had more than 300 million active users and 50% of those users access the site at least once each day (Facebook, 2009a). The amount of time spent on Facebook is also startling; reports indicate that, worldwide, there are more than eight billion minutes spent on Facebook each day (Facebook, 2009a). Facebook consists of a personal profile, where users can provide information about themselves, and the site also includes numerous additional features, such as the ability to add friends, send messages, share photos and create and join groups. There are also privacy features, which enable users to limit access to their account.

Lampe and colleagues (2006) surveyed over 2000 users and found that Facebook was primarily used for social searching. In other words, it is most commonly used to strengthen and maintain existing relationships rather than to meet new people (Ellison, Steinfield & Lampe, 2007). Although Facebook is primarily used for personal purposes, evidence suggests that it also has work related uses (Skeels & Grudin, 2009). For example, employees can use Facebook for professional networking, to obtain and share information, and to advertise products or discuss trends in their field.

Twitter is a micro-blogging service that allows users to provide a short update, of 140 characters or less. The popularity of Twitter has dramatically increased in recent months, with a 3712% increase from April 2008 to April 2009 (Nielson, 2009). Twitter is not only used to provide personal updates, but has also been used for business communications, and by news organisations and political campaigns (Zhao & Rosson, 2009). It can be a useful resource for monitoring trends and changes in any desired area, and for marketing products or services. For example, companies such as Dell use Twitter to provide customers with exclusive offers, and to keep up with customer opinions regarding their organisation, and a number of small businesses utilise Twitter to exploit the digital word-of-mouth that it provides (Miller, 2009).

The predominant SNS used for work purposes is LinkedIn (Wang & Kobsa, 2009). The focus of this site is on professional information; users are encouraged to develop a curriculum vitae and a profile with business related information, such as professional expertise and accomplishments (Skeels & Grudin, 2009). Users can then 'connect' with each other, and can solicit and make recommendations. LinkedIn has over 46 million members, and their mission

[1] http://www.facebook.com
[2] http://www.twitter.com
[3] http://www.linkedin.com
[4] http://www.myspace.com
[5] http://www.youtube.com
[6] The top ranked site is Google Australia

is to "connect the world's professionals to make them more productive and successful" (LinkedIn, 2009).

2.2 Enterprise Social Networking Sites

Enterprise SNS are increasingly popular; these sites differ from general SNS sites because they are internal to an organisation and remain behind the organisation's firewall. This therefore enables employees to communicate and share information with fewer overt privacy risks to the organisation. Although enterprise SNS present fewer security risks, it is important to note that there are limits to their use. For example, they may not support contact with clients, service providers, international counterparts and other external collaborators. Despite this, these tools are likely to be particularly useful in large organisations, where finding and exploiting employees' expertise and knowledge is increasingly difficult. This section of this report briefly describes only some of the enterprise SNS in use.

'Beehive' is an internal site used by IBM employees. It was designed to blur the boundaries between personal and professional life, and to study and understand issues associated with the adoption, usage and impact of these sites within the workplace (DiMicco, Millen, Geyer & Dugan, 2008). Research indicates that most employees use Beehive for professional networking, particularly with those who they believe can assist them with their career goals. Employees also use Beehive to advertise and gather support for their ideas and projects (DiMicco, Millen, Geyer & Dugan, 2008).

IBM also utilise an internal corporate blogging service known as 'BlogCentral'. Huh and colleagues (2007) conducted semi-structured interviews with fourteen active users to investigate the effects of blogging within the workplace. The findings indicated that BlogCentral provides employees with a mechanism to collaborate, give feedback, share expertise and acquire tacit knowledge (Huh et al., 2007).

'WaterCooler' is used internally at Hewlett Packard, and was designed to bring together the various social media tools used within the organisation, with the intention of assisting employees to maintain awareness of new activity (Brzozwski, 2009). These tools include internal versions of Wikipedia and Digg, along with a bookmarking server, a forum server, and a blog server (Brzozwski, 2009). WaterCooler is cross referenced with the employee directory, and allows users to filter information or search based on criteria including topic, popularity and person.

The global communications company BT utilise a number of social media technologies. 'MyBT' is an enterprise social networking tool; similar to SNS such as Facebook, MyBT has features for contacts, message boards, news feeds and social bookmarking (Hill, 2008). It also includes sections that enable employees to record their interests, skills and frequently asked questions, which can assist in the exchange of information and ideas (Hill, 2008).

Present.ly[7] is a micro-blogging tool, and is very similar to the general SNS, Twitter. However, Present.ly is for businesses, and enables users to install the program on their own IT

[7] https://presentlyapp.com/

infrastructure behind a firewall, which provides secure communication and protection from general public dissemination of information. Hence, employees could use this tool to advertise their work projects, or to request advice or assistance with problems.

2.3 Previous Research

Although the use of social networking sites, specifically the use within the workplace, is a relatively new phenomenon, there is still a great deal of predominantly survey-based research in this area.

For example, Acquisti and Gross (2006) surveyed 294 students and staff of a US academic institution regarding Facebook usage and privacy concerns, and this was complemented by an analysis of data mined from the network. Zhao and Rosson (2009) conducted semi-structured interviews with 11 Twitter users, and studied the role that micro-blogging plays in information communication at work. Ross and colleagues (2009) studied personality and motivations associated with Facebook use. Ninety-seven students participated, and completed a measure of personality along with various questions regarding their use of and attitude towards Facebook. Skeels and Grudin (2009) surveyed 430 employees, and conducted semi-structured interviews with 30 people. They studied workplace use of social networking sites, specifically Facebook and LinkedIn.

Steinfield, DiMicco, Ellison and Lampe (2009) studied the use of an internal social networking site, namely, Beehive, which is used by IBM. They surveyed 2435 employees to determine the relationship between the use of Beehive and social capital. DiMicco, Millen, Geyer, Dugan, et al. (2008) conducted semi-structured interviews with 17 Beehive users to study motivations for social networking at work. Brzozwski (2009) examined a year of user behaviour on WaterCooler, which is internal to Hewlett Packard. They also conducted user surveys with 174 users.

More details of these studies as they relate to various areas of interest will be discussed in the following sections of this report.

3. Advantages of Social Networking Sites

There are a number of potential advantages associated with the use of SNS. As well as providing a means to establish and maintain social contacts, these sites provide numerous additional advantages for both personal use and work use (Blackwell, Sheridan, Instone, Schwartz & Kogan, 2009). For example, these sites may provide a useful information resource, and may greatly assist with knowledge sharing. They may also provide emotional support and improve relationships with colleagues, which can help to build rapport.

3.1 Knowledge and Information Sharing

As users are exposed to an escalating amount of data, the ability to locate the most vital information is increasingly important. This information originates from a variety of sources and, particularly in large organisations, finding and utilising the employees' extensive expertise and knowledge can be difficult (Brzozwski, 2009). Although organisations often have methods of sharing official or important information, these methods are unlikely to capture the transient and dynamic nature of employees' knowledge and expertise (Brzozwski, 2009).

SNS may assist with this problem, as these sites enable an organisation to build a distributed knowledge base (Brzozwski, 2009). Although many organisations currently utilise an internal wiki, which has similar functionality, enterprise SNS can enhance this, by improving collaboration, and empowering all employees to share their thoughts and ideas. These sites can also be used to capture both official information and unstructured tacit knowledge, which can allow employees to work more effectively and flexibly. SNS sites could also aid in the rapid resolution of problems, by providing employees with a mechanism to quickly and efficiently access the expertise of many users (Blackwell et al., 2009).

Skeels and Grudin's (2009) survey of 430 employees found that status updates in Facebook assisted some participants to keep up with changes and trends in their field. This was supported by Brzozwski (2009), who found that the micro-blogging component of WaterCooler was often used for requests for assistance. Furthermore, particularly within distributed teams, these status updates could result in faster problem solving, and an increase in team cohesion (Brzozwski, 2009). This study also indicated that SNS can assist users to achieve an understanding of current developments within an organisation, can assist new employees to learn about the organisation, and can assist users to find employees with interests or expertise in specific areas (Brzozwski, 2009).

SNS may also assist organisations to share knowledge and information with clients and customers. These sites can provide a very cheap mechanism to reach an extremely large audience and can also be used to assist an organisation to tailor their message to specific interest groups or demographics (Ofcom, 2008). For example, organisations can use the micro-blogging service, Twitter, to track discussions regarding their brand, and companies can obtain real-time feedback and immediately intervene with any unsatisfied customers (Jansen, Zhang, Sobel & Chowdury, 2009). Furthermore, as alluded to earlier, SNS such as Facebook

enable organisations to set up their own profiles or 'Groups', which can allow users to discuss products and keep up to date with the latest news and information (Ofcom, 2008).

However, it is necessary to note that SNS do significantly increase the amount of information available, and although this information may assist users in some respects, it may also result in information overload. Essentially, time and attention are increasingly scarce resources, and empowering millions of people to share their thoughts not only improves information sharing, but may also result in an unmanageable cacophony of voices (Brzozwski, 2009). This point will be examined in more detail in a subsequent section of this report.

3.2 Improved Relationships

Evidence also suggests that informal relationships with colleagues are vital for sharing organisational knowledge and expertise, and SNS can greatly improve these informal relationships (Steinfield et al., 2009; Hansen, 1999). Furthermore, due to the increase in office automation and the increased frequency of large and distributed organisations, many employees may feel detached, and may have a decreased sense of connection with the organisation's objectives (Brzozwski, 2009).

SNS can help to reduce these problems, by improving employees' relationships and restoring employees' sense of connection (Skeels & Grudin, 2009). Essentially, the use of SNS can assist employees to build rapport with colleagues, which can result in stronger working relationships (Skeels & Grudin, 2009). This not only provides emotional support for employees, but can also create a network of connections that can be utilised to obtain knowledge and expertise, and can also provide opportunities for collaboration (Steinfield et al., 2009; Brzozwski, 2009).

In a survey of 693 Australian workers, 40% of respondents indicated that SNS allow them to network with customers, clients and other employees (Abrahams & McKeon, 2008). This was supported by Zhao and Rosson's (2009) interviews with 11 Twitter users. Participants reported that the site provided them with an opportunity to have 'virtual watercooler' conversations, which enabled employees to learn more about their colleagues, and this then improved professional relationships, and increased knowledge sharing and collaboration (Zhao & Rosson, 2009).

This finding was also supported by Steinfield and colleagues' (2009) study of Beehive users, which found that Beehive enabled employees to strengthen weak ties, and provided users with an opportunity to reach out to employees who they did not know. This was particularly useful for the large number of employees who were located outside of the United States, as the SNS enabled them to develop working relationships with a greater number of people than would have otherwise been possible. The study also indicated that these improved relationships provided benefits to the organisation; Beehive users generally had a greater ability to access expertise and a greater willingness to contribute to the organisation (DiMicco, Millen, Geyer & Dugan, 2008).

There is also evidence to suggest that the content shared on SNS often has very little influence on these benefits. Essentially, sharing information about moods, experiences, successes, failures and interests can improve friendships, and even brief, repetitious and mundane status updates can have positive effects (Skeels & Grudin, 2009). In fact, some research has suggested that people may feel more comfortable asking and responding to personal questions during online interactions, and therefore, SNS may result in stronger relationships than through face-to-face methods alone (McKenna, Green & Glenson, 2002; Tidwell & Walther, 2002). This was supported by a study of college students, which found that greater use of Facebook was associated with stronger relationships with immediate and extended friends (Ellison et al., 2007).

3.3 Work-Life Balance

Related to this, there is also evidence to suggest that personal use of SNS within the workplace may not be entirely detrimental. In fact, the use of SNS may help employees to refresh, which may then have a positive effect on mental health, and may help employees to focus and result in an increase in productivity (Wang & Kobsa, 2009).

An Australian study of 300 workers examined Workplace Internet Leisure Browsing (WILB) and found that employees who spend a reasonable amount of work time using the Internet for personal purposes were approximately 9% more productive (Coker, 2009). This increase in productivity was thought to be associated with peoples' inability to concentrate effectively for long periods of time. Essentially, although employees who take regular breaks may spend less time concentrating on work, they were found to have better concentration, and were therefore capable of higher productivity (Coker, 2009). However, it is necessary to note that, in this study, less than 20% of an employee's time was considered to be within the reasonable limit (Coker, 2009). Hence, for the participants at the high end of this scale, there was still a net loss in production.

Despite this, studies examining the influence of rest breaks on employee performance have also supported the claim that frequent breaks from work can result in beneficial effects in employee productivity and comfort (Balci & Aghazadeh, 2004; Galinsky, Swanson, Sauter, Hurrel & Schleifer, 2000; Koparadekar & Mital, 1994; Mclean, Tingley, Scott & Rickards, 2001).

Allowing SNS at work may also help to increase employee morale and improve the relationship between employers and employees. A survey of 693 full or part time workers in Australia indicated that the vast majority (76%) of respondents believed that allowing employees to use SNS in the workplace provided benefits to the organisation, and of those respondents, 68% felt that allowing these sites showed an element of trust (Abrahams & McKeon, 2008). Furthermore, approximately half of the employees who believed SNS should be permitted in the workplace claimed that the sites provide a break and allow employees to keep fresh (Abrahams & McKeon, 2008).

This survey also indicated that some respondents may make employment decisions based on the ability to access SNS. For example, 46% of those surveyed indicated that they would prefer to work for an organisation that did not block access, and 25% of respondents aged between

16 and 24 indicated that their decision to work for an employer would be influenced by the employer's policy regarding the use of SNS (Abrahams & McKeon, 2008).

However, it is necessary to note that some employees may take advantage of lax rules regarding the use of these sites, and organisational time and money could be lost. Hence, although a work-life balance is important to employees, it is vital to ensure that a firm policy is in place, which will balance the needs of employees with the productivity and security of the organisation.

4. Disadvantages of Social Networking Sites

Although SNS may provide advantages, there are many potential disadvantages and risks, which cannot be ignored. SNS can result in wasted company time, can create tensions within the organisation, and can result in security vulnerabilities. Essentially, many users do not view these sites from a security point of view, and fail to recognise the potential risks.

4.1 Wasted Time

As indicated previously, reports suggest that a vast number of users access SNS during work time (Facetime, 2008), and these sites are predominately used for personal rather than business purposes (Wang & Kobsa, 2009). Hence, within many organisations, the use of SNS during work time is viewed as illegitimate or inappropriate, and the time spent on these sites is deemed to be wasted time (Wang & Kobsa, 2009).

Although Section 3.1 of this report indicated that SNS can greatly assist in knowledge and information sharing, the quality of the information available may be limited, which means that the time spent may not be beneficial. For example, Twitter's 'trends' provide a useful mechanism for discovering what topics are most popular or newsworthy. However, the facts available are generally not verified, which means that the 'real time' dissemination of news contains a great deal of inaccuracies, and therefore, the information available may lack value. Furthermore, these topics are easy to manipulate by spammers, who exploit the popularity of common terms to ensure their spam reaches a wider audience.

There are also a number of employees who believe that SNS are time wasters. A study examining the use of WaterCooler revealed that many employees believed that the benefits gained from utilising these sites were not worth the time and effort (Brzozwski, 2009). Brzozwski (2009) indicated that although some employees enjoy having a 'soap box', and enjoy the act of writing, the majority of employees are under time pressure, and will be unlikely to spend valuable time on these sites unless they are guaranteed that their contributions will be read and valued by others.

Essentially, it is extremely difficult to measure any benefit derived from the use of these sites; they may improve employee support and health, but these factors would (at best) result in indirect benefits to productivity (Skeels & Grudin, 2009). Within a performance-driven culture, it may be difficult to justify the return on investment based on solely indirect benefits (Brzozwski, 2009). Hence, the business use of these sites is likely to be hindered by managerial, organisational and psychological barriers associated with whether using these sites is wasting company time (Brzozwski, 2009).

Interestingly, however, many organisations do not appear to have concerns regarding this wasted time. A recent survey of 555 employees from a range of professions revealed that 86% of organisations use social technologies for business purposes, but 79% of respondents indicated that return of investment is not measured (Mzinga Inc., 2009).

It is also possible to argue that SNS may allow employees to waste less time than other forms of communication. These sites offer 'lightweight' communication without interruption (Skeels & Grudin, 2009). They have voluntary readership, and are less intrusive, as there is less of an expectation for a response than communication modes such as telephone, instant messaging and email (Zhao & Rosson, 2008; Nardi, Schiano & Gumbrecht, 2004). Users can report on their thoughts or experiences as they happen, and 'friends' can check for updates when convenient (Zhao & Rosson, 2008).

Furthermore, it is important to note that researchers once had the same argument in regards to email; it was believed that email was simply a time waster that organisations would remove (Skeels & Grudin, 2009). However, now email is a critical component of most organisations. The same argument was also made in regards to instant messaging, but now many managers and executives use IM for work purposes (Skeels & Grudin, 2009). Hence, it is, perhaps, important to keep an open mind in regards to the usefulness of new or different technologies.

4.2 Risks to Reputation and Confidentiality

There are also risks associated with employees revealing confidential or private information, either about an organisation, or about themselves. This is particularly true of SNS that traverse the company firewall, and for many organisations, the inadvertent disclosure of confidential or proprietary information is a major concern (Skeels & Grudin, 2009; Todd, DiJohn, Aldridge, 2008).

A study by Skeels and Grudin (2009) revealed that many employees discuss company information via ambiguous messages, which are designed to be understood only by knowledgeable work colleagues (Skeels & Grudin, 2009). This is a very risky and dangerous method, as a number of seemingly non-descript status updates could be put together to form a comprehension picture of confidential information.

Furthermore, evidence suggests that SNS can have serious reputation risks, and information shared may not only reflect poorly on the individuals who post inappropriate materials, but may also reflect badly on the organisation. A recent survey of over 3000 hiring managers and human resource professionals indicated that 20% of employers use SNS to research job candidates (Grasz, 2008). Although this research occasionally helped to solidify a hiring decision, the respondents revealed that in more cases they found content that they used to dismiss a candidate from consideration (Grasz, 2008). Hence, sharing too much information or inappropriate information could have important consequences.

Unfortunately, it appears as though many employees do not consider these consequences when revealing information on SNS. Deloitte (2009) conducted a survey examining SNS within the workplace, with a particular emphasis on the risk to reputation associated with utilising such sites. Over 2000 employed adults were surveyed by telephone, and an additional 500 executives took part in an online survey. The results indicated that the vast majority (74%) of employees recognised that a company's reputation could be easily damaged by online activities. However, this knowledge appeared to have little impact on behaviour. For example, more than one-third of respondents indicated that they do not consider their

boss, their colleagues or their clients before posting comments, photos or videos online (Deloitte, 2009).

These dangers are particularly serious, since users tend to lack any realistic sense of the easy access and permanence of any information revealed on the Internet (Rosenblum, 2007). For example, pseudonymous user names on SNS tend to create an illusion that individuals will not be accountable for their behaviour on these sites (Wang & Kobsa, 2009). Many users also fail to recognise the manner in which the meaning of their posts could be distorted without the necessary context (Rosenblum, 2007). Furthermore, users may fail to recognise that their control over information is essentially lost once it has been posted. Generally, the Terms of Service of SNS specify that the site may use any information provided, and hence, even if a user deletes certain information, this information could still be retained by the site. For instance, Twitter's Terms of Service warns that they may "use, copy, reproduce, process, adapt, modify, publish, transmit, display and distribute" posts (Twitter, 2009).

As demonstrated by a recent court case, behaviour on these sites could also have legal ramifications. In this case, an Adelaide man was convicted of criminal defamation after posting information about a police officer on Facebook (Hunt, 2009). This case has now set a legal precedent, and it is also possible that employee behaviour on these sites could have legal ramifications for organisations. If defamation, bullying, discrimination or harassment takes place, and an organisation had provided a platform to allow external posts and failed to put in place an associated policy, then it could be argued that an organisation has some legal liability (Park, 2008). Furthermore, if employees use these sites within the workplace and access objectionable or offensive content, it could be argued that the employer had some responsibility to protect the employee from viewing such material (Kelleher, 2009). Although (at the time of writing this report) an organisation's potential liability has not yet been tested, these are still important issues that organisations should not ignore.

4.3 Disruptions to the Working Environment

Evidence also suggests that the use of SNS can cause disruptions to the working environment (Todd et al., 2008). These disruptions are often caused by mixing different types of contacts, such as work contacts and personal contacts, and tensions can also result in crossing the power boundaries that exist within an organisation (Skeels & Grudin, 2009; Wang & Kobsa, 2009). Binder, Howes & Sutcliffe (2009) claim that this is a problem associated with peoples' fundamental need to maintain independent social spheres.

Essentially, there are usually differences in the manner in which users communicate with people from different social spheres. For example, a topic that would be openly discussed with close friends may not be appropriate for a discussion with a senior manager. In the real world, these boundaries are usually clear, but evidence suggests that SNS often lack these rules and social conventions, and generally fail to provide a mechanism to deal with this issue (Ofcom, 2008). There is also research examining the meaning, implication and impact of the 'friending' function within SNS, which can also result in social drama and tension (Boyd, 2006). This problem can occur because the meaning of 'friends' on these sites is not necessarily the same as the everyday sense of the word, and also because it can mean different things to different people.

Skeels and Grudin (2009) examined the implications of crossing social boundaries in SNS, and their research revealed that users often felt obligated to accept friend requests from their clients and other professional contacts. Participants expressed similar feelings of obligation in regards to senior management; users may not wish to share personal information with these work colleagues, but may not want to risk offending a superior by refusing the request. Generally, these obligated connections cause people to restrict the information that they disclose, which can then result in frustration, irritation and feelings of resentment (Skeels & Grudin, 2009). Alternatively, people may not alter their behaviour, which could result in risks to their reputation.

Binder and colleagues (2009) surveyed over 200 Facebook users and, although the respondents reported tensions associated with the presence of different social spheres, there was no evidence that the number of work contacts resulted in an increase in online tension. However, the authors suggested that tensions in this area could be more associated with the specific work contacts rather than the number of work contacts (Binder et al., 2009). In other words, a work contact who is subordinate or a superior is more likely to result in social tensions.

4.4 Security Vulnerabilities

There are also many security vulnerabilities associated with the use of SNS. Most users do not consider security or privacy, and the perceived anonymity associated with these sites can result in a false sense of security. Furthermore, evidence suggests that many people are too trusting, and tend to trust by default (Hamiel & Moyer, 2008). Hence, users can expose themselves (and often their organisation) to a number of potentially serious security vulnerabilities.

Essentially, many users seem to assume that they are protected on these sites, and many users fail to exercise the same level of common sense that they would exercise in the real world (Rosenblum, 2007). As in the real world, SNS are composed of a mix of people, including not only trustworthy people, but also dishonest people (Greiner, 2009). Unfortunately, many users fail to recognise that the information that they reveal on these sites can be used by people with malicious intentions for nefarious purposes, including stalking, identity theft and other self-interested reasons. For example, an individual could masquerade as a like-minded or similarly connected person in order to obtain information from a SNS, and the information obtained could be used to exert pressure on an individual to reveal company secrets.

A number of researchers have revealed that people often share too much information on these sites, and privacy concerns often have little impact on behaviour (Acquisti & Gross, 2006). For example, Acquisti and Gross (2006) conducted a study with over 500 participants, and revealed that there was no relationship between self-reported privacy concerns and the tendency to reveal personal information. Participants were asked to rate their level of privacy concerns regarding strangers knowing their schedule of classes and where they lived, and the participants were then asked if they shared this information on Facebook. Of the 16% of participants who reported the highest level of privacy concerns, 22% provided their home address, and 40% provided their schedule of classes (Acquisti & Gross, 2006).

Furthermore, Gross, Acquisti and Heinz (2005) examined 4540 Facebook profiles from Carnegie Mellon University students and found that a great deal of information is regularly shared. In this sample, 91% of profiles contained an image, 88% of users revealed their birth date, 40% revealed a phone number and 51% revealed their current residence. Furthermore, most users also exposed information regarding their relationship status, dating preference, political views and other interests (Gross et al., 2005). Although these results are from 2005, and are therefore not necessarily still an accurate representation of current behaviour, they do reveal a trend towards sharing personal information via SNS.

More recent studies have indicated that fewer users reveal sensitive information, and more users tend to place restrictions on the access to their personal page (Ofcom, 2008). For example, a study from the United Kingdom indicated that 44% of users had no restrictions on who could view their profile, and 48% had restricted access to only users within their list of friends (Ofcom, 2008). A similar study by Fogel and Nehman (2009) found that only 9% of participants revealed their home address and phone number. However, in this study, the vast majority of people (74%) had no restrictions on who could view their profile, and 86% included an image (Fegel & Nehman, 2009). This therefore still suggests that people are very trusting.

Many users of SNS are also very trusting regarding the people who they are willing to add as 'friends'. This was demonstrated by Charlie Rosenbury, who was a computer-science student at the University of Missouri (Schwartz, 2005). Rosenbury wrote a program to automate the process of adding people as 'friends' on Facebook, and then sent messages to 250,000 users. Over 70,000 users agreed. The IT security company, Sophos, conducted a similar exercise to highlight the dangers of irresponsible behaviour on SNS (Sophos, 2007). They created a fabricated Facebook profile, with minimal personal information, and then sent friend requests to 200 Facebook users. The request was accepted by 87 users, and over 94% of those users provided access to personal information, such as their date of birth, address or location and phone number.

Evidence also suggests that people who reveal information on SNS can be vulnerable to social engineering attacks. Jagatic, Johnson, Jakobsson and Menczer (2007) conducted a study that revealed the vulnerabilities associated with SNS, and indicated that information from these sites can be used for social engineering. They used publicly available sites such as Facebook to discover social networks, and then launched actual phishing attacks on 921 Indiana University students. Half of the participants acted as a control group, and received emails from a fictitious email address. For the remainder of the participants, the information gathered from social networks was used, and these participants were sent emails that appeared to be from a friend. The success rate for the participants in the control group was 16%, and this increased to 72% when the phishing attack appeared to originate with a member of the participants' social network. The study therefore revealed that the people were far more vulnerable to such attacks when social context was utilised (Jagatic et al., 2007). Hence, this indicates the dangers associated with revealing information on SNS.

Associated with this, the lack of identity verification on these sites is also a very serious problem, particularly for sites such as LinkedIn that are used primarily for business purposes

(Hamiel & Moyer, 2009). Hamiel and Moyer (2009) revealed a number of the security vulnerabilities associated with SNS. With permission from the individual impersonated, the authors created a fake LinkedIn profile for a well-known security leader and in less than 24 hours, they were able to obtain more than 50 connections. These connections included federal employees, the chief security officer of a security firm and family members of the impersonated individual. As indicated in the paragraph above, social engineering attacks are far more effective when they appear to originate from a trusted source. Hence, if links to a new website or application had been sent from the faked LinkedIn account, the likelihood of people following these links would be far higher than an anonymous phishing attack (Hamiel & Moyer, 2008). Furthermore, since the impersonated individual was a well-known security leader, people were also more likely to discuss security sensitive information with him (Rosenblum, 2007). Essentially, it is extremely difficult to police the validity of accounts, and hence, it is dangerous to presume that an individual is who he or she claims to be (Rosenblum, 2007).

There are a number of similar cases, where fraudulent individuals have pretended to be someone else for profit (Sutter & Carroll, 2009). For example, in January 2009, the status update of Facebook user Bryan Rutberg became a plea for help, and an online friend received a direct message, saying that Rutberg had been robbed in London, and needed money to return home (Greiner, 2009). The friend sent over $1000 to Rutberg's London address. However, unbeknownst to the friend, Rutberg's Facebook account had been hacked, and Rutberg was safely at home (Sutter & Carroll, 2009). Research indicates that people are more likely to succumb to social engineering attacks when they are in a heightened emotional state, and hence, strategies such as the one that defeated Rutbery's friend are likely to be particularly successful (Parsons, McCormac, Butavicius & Ferguson, 2010; Gragg, 2002).

An increasing number of SNS also allow third party applications, which are extremely varied in their style and purpose, and can result in a number of serious security threats (Felt & Evans, 2008). Statistics indicate that these applications are extremely common; over 70% of Facebook users engage with them, and more than 350 applications have more than one million active users each month (Facebook, 2009a). Furthermore, more than one million people from more than 180 countries are developers of these applications.

In order to operate, users are often required to agree to release sensitive content about themselves and their friends. For example, one commonly used third party application on Facebook requires users to agree that they allow the application to "access your Profile information, photos, your friends' info and other content that it requires to work" (Facebook, 2009b). There is no immediately identifiable list of the information that the application will require, and it is not clear if this includes the information of friends who have restricted the access to their profile. However, the act of clicking 'yes' is such a habitual activity for most computer users that the majority of people are likely to agree without considering the consequences (Parsons et al., 2010). Since these applications are, in most cases, made by an unknown person, this means that most people would have no idea with whom they are sharing information.

According to Hamiel and Moyer (2008), these third-party applications can be particularly problematic, as seemingly legitimate widgets can 'go rogue' after spreading to a certain

number of members. These applications are usually developed by individuals with very little security or programming knowledge, and in many cases, people may unknowingly create their applications with vulnerabilities that a malicious user could exploit (Hamiel & Moyer, 2008). However, as SNS have an end user licence agreement that absolves them of all responsibility for third party applications, there is little incentive for sites to effectively police the quality of these applications (Hamiel & Moyer, 2008). Furthermore, many users feel that because they do not have to install anything on their computer, they do not have to worry about viruses or malware (Hamiel & Moyer, 2008). Hence, users may not apply an adequate level of caution.

Due to this inadequate level of caution, hacking SNS can be alarmingly easy. For example, Facebook and MySpace have been infected by the malware called 'Koobface', which took advantage of users' tendency to trust their friends (Greiner, 2009). Victims of this malware received a message that appeared to originate from a friend, with instructions to follow a link to a video. The message often claimed that the link was to an embarrassing or funny video of the victim, and therefore, the chance of the victim following the link was extremely high. Clicking on the link would present the victim with an alert, claiming that it was necessary to download an updated version of Flash Player (Better Business Bureau, 2009). However, in reality, the update installed a Trojan onto the victim's computer (Greiner, 2009).

Unfortunately, there are many stories such as this, where thieves, scam artists and hackers have used SNS for personal gain. Essentially, users who place too much trust in these sites are likely to have this trust compromised (Greiner, 2009). It is also important to note that, although most SNS have privacy options, they are unlikely to be infallible. Instead, it is highly likely that knowledgeable hackers or malicious insiders could circumvent the protections. This could be done through technical means (e.g., hacking into a network), or through non-technical means (e.g., social engineering). It is therefore vital to ensure that users have adequate security awareness.

5. Suggestions for Security Awareness

Although the advantages of SNS may help to validate their use, the potential risks and disadvantages are very serious, and hence, it is vital to ensure that users have an adequate awareness of any security threats. Unfortunately, the majority of users appear to have a lack of knowledge of these issues.

A number of studies have revealed that most users either do not consider the security and privacy implications, or have a limited understanding of the potential security risks and other consequences associated with SNS (Ofcom, 2008; Acquisti & Gross, 2006; Krishnamurthy & Wills, 2008). For example, many users presume that only people within their friendship network can view their details (Ofcom, 2008). Furthermore, many users are unaware of the public and permanent nature of any information shared on SNS (Rosenblum, 2007).

It is therefore important to educate employees regarding the potential consequences, to ensure that behaviour on these sites minimises any possible risks to individuals and to their organisations. It is also important for organisations to develop an appropriate policy regarding the use of these sites, which should also help to minimise the risks to organisations.

5.1 The Importance of a Policy Regarding SNS

It is vital for organisations to determine whether the use of SNS will be forbidden, tolerated or encouraged, and an associated policy should then be developed (Park, 2009). However, because technology in this area is constantly changing, it is important to ensure that the policy is not too specific, as a very specific policy may quickly become obsolete. Despite this, an effective policy is important, as it should help to increase certainty for employees and reduce risks for the organisation (Park, 2009). It is also important to ensure that any policy specifies both enterprise and general SNS, as the rules associated with these types may differ greatly. For example, enterprise SNS might be a valued knowledge management resource, whose use should be encouraged, whereas the use of general SNS might be governed by a far more stringent acceptable use policy.

Furthermore, a number of aspects of general SNS may be governed by an acceptable behaviour policy. Essentially, many of the issues identified in this report not only relate to SNS, but also relate to employee behaviour in general. For example, regardless of the setting, the public behaviour of employees can reflect badly on an organisation, and it is always important to ensure that employees do not share confidential information. Hence, the combination of an acceptable use policy and an acceptable behaviour policy should cover many of the issues associated with SNS.

However, although those policies may implicitly cover the use of SNS, it is still important to more explicitly outline employees' obligations, and identify any gaps in the current policy (Sherry, 2008). The policy should cover issues associated with defamation, intellectual property, estoppel, public relations, confidential and proprietary information, and misleading and deceptive conduct (Park, 2009). It should also specify both the possible legal ramifications associated with the use of SNS and any non-legal aspects.

An effective policy should be supported by an initial education and training program, regular refresher training and information regarding the consequences associated with a failure to comply (Park, 2009). It may also be appropriate to supplement an effective policy with technical solutions, such as intrusion detection and prevention systems to monitor network traffic (Sherry, 2008). Furthermore, it is important to not only describe the details of the policy, but to also stress the reasons why adherence is important.

Unfortunately, evidence suggests that few organisations have appropriate policies regarding the use of these sites, and employees' understanding of the policies that do exist is generally poor (Deloitte, 2009). For example, a survey of SNS within the workplace indicated that 24% of respondents did not know whether their organisation had a policy for the use of these sites. An additional 23% of employees indicated that their organisation did not have a policy, and a further 11% did not know what the policy comprised (Deloitte, 2009).

These statistics are supported by a survey of executive level employees, in which only 22% of respondents said that their company had formal policies to dictate the use of SNS (Deloitte, 2009). Furthermore, very few (17%) organisations had programs in place to monitor and mitigate risks associated with the use of SNS, which means that organisations may not be aware of the existence of potentially damaging information (Deloitte, 2009).

5.2 The Importance of Education

Even more alarmingly, Deloitte's (2009) survey revealed that a company policy would not change online behaviour for 49% of employees. This therefore highlights the importance of education; many individuals are currently unaware of the potential risks associated with SNS, and are therefore unlikely to change their behaviour. It is necessary to improve employee education regarding the use of SNS, to ensure that employees are able to make informed and rational decisions.

A number of important factors associated with security awareness training and education are outlined in Parsons et al. (2010). Essentially, training programs are more likely to be successful if the learning is personal, meaningful, contextualised, and regularly reinforced. Hence, training should be tailored towards the intended audience to ensure that the needs of individuals are considered.

Evidence suggests that case studies are a very effective method of communicating a message to an audience (McIlwraith, 2006). Case studies generally involve providing specific, real-life examples, and the value of this method of training has been demonstrated by Herreid (1994), who revealed an increase in lecture attendance from 50-65% for traditional lectures to 95% when case studies were utilised. Hence, an effective education program should provide case studies demonstrating the sorts of information that can be quickly obtained from SNS and examples of the negative ways in which any obtained information could be utilised.

This method is particularly important, because security awareness is often a secondary concern for employees. In many organisations, employees are under great pressure to achieve more and more with fewer and fewer resources, and in such a performance driven culture, the

most real and important risks are the risks associated with not getting the job done (Schneier, 2009). In other words, the consequences of not following security policies may seem less serious than the consequences of not completing a project on time. Hence, lecturing employees regarding the security policies that they are required to follow is unlikely to be as effective as case studies, where employees are provided with actual events where the non-adherence of policy resulted in negative consequences. Simply put, education and training programs need to be implemented effectively to have a significant impact on behaviour (Parsons et al., 2010).

5.3 Recommendations for Security Awareness on SNS

This section provides an overview of a number of recommendations for security awareness in regards to SNS. It is important to ensure that employees are informed of the security and privacy implications of their interactions on SNS. They should be encouraged to stop and think before posting any information on the Internet, and any information that people do not want in the public arena should not be posted on these sites (Park, 2009). It is also important to avoid posting when angry or in a hurry, to avoid sarcasm and fights, and to always treat readers with respect (Park, 2009). If individuals are provided with information such as this, they should then be able to make informed and rational decisions regarding the use of these sites, which should help to minimise risk.

Employees should also be provided with information that specifically relates to the possible impact upon an organisation. Park (2009) provides a number of best practice guidelines, designed to encourage compliance, and minimise risks to individuals and organisations. The users of SNS should be encouraged to consider the impact that any information could have on the reputation of their organisation, or on their own reputation (Park, 2009). They should also be warned against speaking on behalf of their employer, and they should ensure that their language does not imply that they are speaking on an organisation's behalf. Furthermore, employees should be warned that their employer may monitor their activities, and they should not use a company email address when joining these sites (Park, 2009). It is also important to emphasise employees' confidentiality obligations; employees should be cautious when sharing any company activities, and should be warned to never reveal confidential information, even on a password protected SNS (Park, 2009).

The users of SNS should also be encouraged to utilise the privacy options provided by sites, which restrict access to authorised personnel only. These privacy settings are often very powerful, and can provide a wide range of options for users to display or limit various aspects of their page to specified people (Bonneau & Preibusch, 2009). For example, Facebook has functionality to allow users to create groups of people, and then choose which groups can access their information and applications. This could enable users to effectively manage the potential problems associated with mixing different types of friends; work colleagues could be permitted to view only information that presents a professional image, and information of a private nature could be restricted to only close friends.

However, the privacy settings available on these sites are often very counterintuitive and complicated, and are often difficult to find (Strater & Lipford, 2008). Bonneau and Preibusch (2009) evaluated the privacy options offered by various SNS, and concluded that information

regarding privacy is generally lacking. In addition, the various sites generally utilise different terminology for their privacy controls, which further increases the effort involved to understand and implement these privacy settings (Bonneau & Preibusch, 2009).

Facebook recently made changes to their privacy controls, which were designed to simplify the settings, and give users more control over their information (Bankston, 2009). However, an analysis of these changes indicates that they actually *reduced* users' ability to control their personal data, and were clearly intended to *increase* the amount of publicly shared information (Bankston, 2009). Related to this, as indicated in Section 4.4, a vast number of users do not alter the default privacy settings (Ofcom, 2008; Fogel & Nehman, 2009), and, by default, most sites share all profile information (Hamiel & Moyer, 2009).

Ideally, SNS should have better default settings. However, although organisations may not have the ability to control this, they can educate their employees to ensure that they know how to find and use the settings, and how to tailor the settings for different purposes. This should then minimise the chance that SNS will result in inadvertent privacy risks and tensions.

It is also vital for employees to follow good password practices, to minimise the chances of having their account hacked. This includes using a unique password for each site, and employees should also be encouraged to use different passwords for personal sites than for work-related sites. Furthermore, employees should be cautious if using password reset questions, and should ensure that the answer to the question is not shared on a SNS. For example, password reset questions often require information such as an individual's home town, a pet name, or mother's maiden name, which is all information that could be shared on a SNS.

It is also important to stress that users should be cautious and sceptical when utilising SNS. People should think carefully about whether to add someone as a friend, particularly if the request is from a stranger (Sophos, 2009). Also, although SNS are about sharing information, users should think carefully about which information to share, and should strongly consider keeping information such as phone numbers and addresses private (Better Business Bureau, 2009). Rosenblum (2007) also suggests that people should periodically review what information is available about them online. Similarly, users should review who has access to their SNS, and should be willing to update and modify this where necessary.

Users should also be warned to display caution regarding messages that contain links to external sites, and users should also be cautious regarding any other suspicious messages, even if the message appears to originate from a friend. For example, if a user receives a message from a friend requesting money, the Better Business Bureau (2009) recommend that people should first contact the friend via a means other than the SNS, and, if that is not possible, they should attempt to verify their friend's identity by asking a question that only the friend could answer (ensuring that the answer is not available on the friend's SNS).

It is also important to evaluate any site before joining, and to maintain awareness of the privacy policy and Terms of Service. This is vital, as these are regularly changed by the site, which can alter the manner in which the company controls and protects data (Better Business

Bureau, 2009). Furthermore, SNS should only be used on a computer with a reliable firewall and current antivirus software, and users should be cautious regarding the installation of any third-party applications (Better Business Bureau, 2009).

These recommendations constitute a considerable amount of information for employees to comprehend. Although it is necessary to provide employees with extensive information regarding the use of these sites, it is also important to ensure that they are not overwhelmed by too much information. As mentioned previously, a worrying percentage of employees claimed that they would not change their behaviour to meet a company policy (Deloitte, 2009), and it is therefore vital to ensure that the risks associated with SNS and the necessary precautions are communicated in an effective manner. It is also important to continue to monitor changes in SNS, and, when sites change, it may be necessary to modify or adapt any policies and education programs to ensure that they remain appropriate.

6. Suggestions for Future Research

One of the most difficult factors associated with researching SNS is the speed with which this area changes. The existence and popularity of sites is so dynamic that developing and undertaking a study that will remain valuable once completed is a non-trivial matter. There are, however, still many possible areas of research that should be investigated in the future.

Arguably the most crucial area of research would involve a comprehensive investigation of the business value of these sites. As indicated in Section 3 of this report, a number of researchers have suggested that SNS can provide benefits to organisations. However, there is insufficient research attempting to quantity these benefits, and there is a distinct lack of research examining the return on investment associated with the use of these sites. Although this is a very difficult area to research effectively, many organisations will be hesitant to permit employees to spend time on SNS until it can be proven that this time provides a quantifiable benefit to the organisation.

Research in this area should attempt to better understand how social collaboration can assist employees, together with a thorough investigation of which social networking tools are the most useful in a business setting, and which tools are the most distracting (Blackwell et al., 2009). Similarly, it is also important to research the best integration strategies, which would maximise the benefits derived from these sites without jeopardising the productivity of the organisation.

Additionally, although some researchers have examined the benefits of enterprise SNS, and others have studied the effects of general SNS, what is crucial is a thorough comparative study, investigating the impact of both types of sites on particular organisations. For example, are factors such as risk, productivity and job satisfaction influenced more by one type than the other, and are these factors likely to differ between various organisations? Also, will these factors be more influenced if a tool was implemented within an organisation's current systems, or should these tools stand alone (Blackwell et al., 2009)?

Furthermore, it is also important to study which factors are likely to influence the adoption of these sites. A study of WaterCooler (the enterprise site used within Hewlett Packard) found that the site was used by only a small proportion of employees, and, ironically, the reason why many employees were not using the site was due to the small participation rate (Brzozwski, 2009). It is therefore vital to develop methods to support and improve the adoption of enterprise SNS.

Studies of SNS should also include a better sample of employees, as many previous studies have only included the users of these sites (Wang & Kobsa, 2009). For example, a study by DiMicco and colleagues (2009) examined the use of Beehive, and found that employees did not have any privacy concerns towards this site. However, the study only included the users of this site, and therefore the findings are not necessarily representative of most employees. Future studies should also include the employees who do not utilise these sites at work, to obtain an understanding of why they do not use the sites, and whether any changes would encourage them to use SNS in the future (Wang & Kobsa, 2009).

It would also be useful to further research the effectiveness of different modes of risk communication. As indicated in this report, a large proportion of the users of SNS either do not recognise the security risks associated with the use of these sites, or are not willing to change their behaviour to mitigate these threats. Hence, it is vitally important to develop effective education campaigns, and it would be extremely useful to assess a variety of different modes of communication, to obtain insight into the most successful methods.

Similarly, it would also be useful to assess risk-taking behaviours and personality attributes to determine whether these aspects are associated with SNS usage. For example, are any personality characteristics associated with an individual's propensity to share information on these sites? Furthermore, are people who rate highly on measures of risk-taking behaviour more likely to share information on these sites?

The research undertaken could take a number of forms. A qualitative research project within departments of the Australian Government could involve interviews with employees from a number of organisations to obtain a comprehensive understanding of the manner in which these sites have impacted upon the employees' lives, and the ways in which employees feel that these sites could benefit their working lives. A quantitative research project could also be undertaken, which could involve an analysis of computer logs and publicly available information on SNS to obtain statistics on the amount of time currently spent on SNS, and the types of information that employees currently reveal. A survey technique could combine both qualitative and quantitative methods, to efficiently study the attitudes and past behaviours of a large number of participants, providing a more valid and detailed knowledge of the ways in which SNS influence the workplace dynamic.

7. Conclusions

This report has highlighted the importance of a thorough understanding of the implications of SNS. Although these sites may provide a number of benefits, such as improved knowledge sharing and improved relationships, this report has also highlighted the many potential risks associated with the use of these sites. For example, SNS can waste company time, can disrupt the working environment, and can jeopardise privacy, security and confidentiality in a number of ways. Furthermore, previous studies have indicated that many users of these sites do not consider security or privacy, which further increases the risk to organisations.

Despite these potential problems, SNS are continuing to grow at a rapid rate. For the generation currently studying to become professionals in workplaces around the world, these sites are becoming an integral part of life. Evidence also suggests that the fastest growing demographic on SNS is those over 35 years of age (Facebook, 2009a). Hence, it is increasingly important for organisations to decide whether the benefits provided by these sites outweigh the potential costs (Skeels & Grudin, 2009). Abrahams and McKeon (2008) suggest that organisations need to learn to manage these risks, as they have for previous technologies such as email and instant messaging.

It is therefore vital for organisations to develop a clear and enforceable policy regarding the use of these sites, which should be coupled with a personal, meaningful and contextualised education campaign. Such a campaign is likely to be particularly effective if case studies are utilised. This should help to ensure that employees are able to make informed and rational decisions regarding the use of these sites, and should then minimise the chance of negative consequences. Simply put, SNS may provide an abundance of potential opportunities, but these opportunities must be weighed with the variety of risks and vulnerabilities.

8. Reference List

Abrahams, N. & McKeon, P. (2008). *Media release: Employers taking chances when blocking Facebook too, says Deacons*. Deacons. Retrieved September 2009, from http://www.deacons.com.au/legal-services/technology-media-telecommunications/media-releases/media-release.cfm?objid=6383

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. *Proceedings of the 6th Workshop on Privacy Enhancing Technologies (PET)*, June 28, 2006, Cambridge, England.

Alexa (2009) *Alexa: The Web Information Company*. Retrieved September 2009, from http://www.alexa.com

Balci, R. & Aghazadeh, F. (2004). Effects of exercise breaks on performance, muscular load, and perceived discomfort in data entry and cognitive tasks. *Computers and Industrial Engineering, 46*, 399-411.

Bankston, K. (2009). *Facebook's New Privacy Changes: The Good, The Bad, and The Ugly*. Electronic Frontier Foundation, Retrieved December 2009 from http://www.eff.org/deeplinks/2009/12/facebooks-new-privacy-changes-good-bad-and-ugly

Better Business Bureau (2009, January 5). *BBB warns: Your Facebook friends could actually be hackers, scam artists, and ID thieves*. Retrieved August 2009, from http://www.bbb.org/us/article/8556

Binder, J., Howes, A. & Sutcliffe, A. (2009). The problem of conflicting social spheres: Effects of network structure on experienced tension in social network sites. *Proceedings of the 27th International Conference on Human Factors in Computing Systems*, Boston, MA: ACM Press, 965-974.

Blackwell, J., Sheridan, J., Instone, K., Schwartz, D.R. & Kogan, S. (2009). Design and adoption of social collaboration software within businesses. *Proceedings of the 27th International Conference Extended Abstracts on Human Factors in Computing Systems*, Boston, MA: ACM Press, 2759-2762.

Bonneau, J. & Preibusch, S. (2009). The privacy jungle: On the market for data protection in social networks. Proceedings of the Eighth Workshop on the Economics of Information Security, London, UK.

Boyd, D. (2006, December 4). Friends, Friendsters, and MySpace Top 8: Writing community into being on social network sites. *First Monday, 11(12)*. Retrieved October 2009, from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1418/1336

Boyd, D. & Ellison, N. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication, 13(1)*, 210-230.

Brzozwski, M.J. (2009). WaterCooler: Exploring an organization through enterprise social media. *Proceedings of the 2009 International Conference on Supporting Group Work*, Sanibel Island, FL, USA: ACM Press, 219-228.

Coker, B. (2009, April 2). *Freedom to surf: Workers more productive if allowed to use the internet for leisure*. Media release, The University of Melbourne. Retrieved September 2009, from http://voice.unimelb.edu.au/news/5750/

Deloitte (2009). *Social Networking and Reputational Risk in the Workplace: Deloitte LLP 2009 Ethics & Workplace Survey Results*. Deloitte Development LLC.

DiMicco, J., Geyer, W., Millen, D., Dugan, C. & Brownholtz, B. (2009). People sensemaking and relationship building on an enterprise social network site. *Proceedings of the 42nd Hawaii International Conference on System Sciences*, Hawaii, USA: IEEE Computer Soceity, 1-10.

DiMicco, J., Millen, D.R., Geyer, W., Dugan, C., Brownholtz, B., & Muller, M. (2008). Motivations for social networking at work, *Proceedings of the ACM 2008 Conference on Computer Supported Cooperative Work*, San Diego, CA, USA: ACM Press, 711-720.

DiMicco, J.M., Millen, D.R., Geyer, W. & Dugan, C. (2008). Research on the use of social software in the workplace. *Position paper presented at the ACM 2008 Conference on Computer Supported Cooperative Work*, November 8-12, San Diego, CA.

Ellison, N.B., Steinfield, C. & Lampe, C. (2007). The benefits of Facebook "Friends": Social capital and college students' use of online social network sites. *Journal of Computer Mediated Communication, 12(4)*, 1143–1168.

Facebook (2009a). *Statistics | Facebook*. Retrieved October 2009, from http://www.facebook.com/press/info.php?statistics

Facebook (2009b). *Facebook*. Retrieved October 2009, from http://www.facebook.com

FaceTime (2008, October). *The Collaborative Internet: Usage Trends, End User Attitudes and IT Impact*. Fourth Annual Survey, FaceTime Communications.

Felt, A. & Evans, D. (2008). Privacy protection for social networking APIs. *Proceedings of the 2009 IEEE/ACS International Conference on Computer Systems and Applications*, Rabat, Morocco: IEEE Computer Society, 1-8.

Fogel, J. & Nehman, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior, 25*, 153-160.

Galinsky, T.L., Swanson, N.G., Sauter, S.L., Hurrel, J.J. & Schleifer, L.M. (2000). A field study of supplementary rest breaks for data-entry operators. *Journal of Ergonomics, 43(5)*, 622-638.

Gragg, D. (2002). *A Multi-Level Defense Against Social Engineering*. White paper, SANS Institute, Retrieved June 2008, from http://www.sans.org/rr/papers/51/920.pdf

Grasz, J. (2008). *One-in-Five Employers Use Social Networking Sites to Research Job Candidates, CareerBuilder.com Survey Finds*. Retrieved September 2009, from http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr459&sd=9%2f10%2f2008&ed=12%2f31%2f2008&siteid=cbpr&sc_cmp1=cb_pr459_

Greiner, L. (2009). Hacking social networks. *Networker, 13(1)*, 9-11.

Gross, R. Acquisti, A. & Heinz, H.J. (2005). Information revelation and privacy in online social networks. *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, Alexandria, VA, USA: ACM Press, 71-80.

Hamiel, N. & Moyer, S. (2009). Fail 2.0: Further musings on attacking social networks. *ShmooCon 2009*, Washington DC.

Hamiel, N. & Moyer, S. (2008). Satan is on my friends list: Attacking social networks. *Blackhat*, Las Vegas, NV.

Hansen, M.T. (1999). The search-transfer problem: The role of weak ties in sharing knowledge across organization subunits. *Administrative Quarterly, 44(1)*, 1143-1168.

Herreid, C.F. (1994). Case Studies in Science – A Novel Method of Science Education. *Journal of College Science Teaching 23(4)*, 221–229.

Hill, A. (2008). *BT Enterprise 2.0: Social Media Tools as an Aid to Learning and Collaboration in the Workplace, for the Digital Generation and Beyond*. Digital Generation Case Study, Career Innovation. Retrieved September 2009, from, http://richarddennison.files.wordpress.com/2008/09/ci-digital-generation-bt.pdf

Huh, J., Jones, L., Erickson, T., Kellogg, W., Bellamy, R. & Thomas, J. (2007). BlogCentral: The Role of Internal Blogs at Work. *Proceedings of the CHI'07 Extended Abstracts on Human Factors in Computing Systems*, San Jose, CA: ACM Press, 2447-2452.

Hunt, N. (2009, November 22). Teen guilty of Facebook slur. *Adelaide Now*, Retrieved November 2009 from http://www.news.com.au/adelaidenow/story/0,22606,26381751-5006301,00.html

Jagatic, T.N., Johnson, N.A., Jakobsson, M. & Menczer, F. (2007). Social phishing. *Communications of the ACM, 50(10)*, 94-100.

Jansen, B.J., Zhang, M., Sobel, K. & Chowdury, A. (2009). Micro-blogging as online word of mouth branding, *Proceedings of the 27th International Conference Extended Abstracts on Human Factors in Computing Systems*, Boston, MA: ACM Press, 3859-3864.

Java, A., Song, X., Finin, T. & Tseng, B. (2007). Why we twitter: Understanding micro-blogging usage and communities. *Proceedings of the International Conference on Knowledge Discovery and Data Mining*, San Jose, CA: ACM Press, 56-65.

Kelleher, D. (2009, October 5). 5 problems with social networking in the workplace. Information Management Special Reports. Retrieved October 2009, from http://www.information-management.com/specialreports/2009_165/social_networking_media-10016208-1.html

Koparadekar, P. & Mital, A. (1994). The effect of different work-rest schedules on fatigue and performance of a simulated directory assistance operator's task. *Ergonomics, 37(10)*, 1697-1707.

Krishnamurthy, B. & Wills, C.E. (2008). Characterizing privacy in online social networks. *Proceedings of the First Workshop on Online Social Networks*, Seattle, WA: ACM Press, 167-170.

Lampe, C., Ellison, N. & Steinfield, C. (2006). A face(book) in the crowd: social searching vs. social browsing, *Proceedings of the 2006 20th Anniversary Conference on Computer Supported Cooperative Work*, Banff, Alberta, Canada: ACM Press: 167-170.

LinkedIn (2009). *LinkedIn – Public Relations.* Retrieved September 2009, from http://press.linkedin.com/about

McFedries, P. (2007). Technically speaking: All a-twitter. *IEEE Spectrum, 44(10)*, 84.

McIlwraith, A. (2006). Information Security and Employee Behaviour: How to Reduce Risk Through Employee Education, Training and Awareness. Aldershot, UK: Gower Publishing Limited.

Mclean, L., Tingley, M., Scott, RN. & Rickards, J. (2001). Computer terminal work and the benefit of micro-breaks. *Applied Ergonomics, 32(3)*, 225-37.

McKenna, K.Y.A., Green, A.S. & Glenson, M.E.J. (2002). Relationship formation on the Internet: What's the big attraction? *Journal of Social Issues, 58(1)*, 9–31.

Miller, C.C. (2009, July 22). Marketing small businesses with Twitter. *New York Times*, Retrieved September 2009, from http://www.nytimes.com/2009/07/23/business/smallbusiness/23twitter.html

Mzinga, Inc. & Babson Executive Education. (2009). *Survey: Social Software in Business*, September 2009.

Nardi, B.A., Schiano, D.J. & Gumbrecht, M. (2004). Blogging as social activity, or, would you let 900 million people read your diary? *Proceedings of the 2004 ACM Conference on Computer Supported Cooperative Work*. Chicago, Illinois, USA: ACM Press, 222–231.

The Nielson Company (2009). *Time spent on Facebook up 700 percent, but MySpace.com still tops for video, according to Nielsen*. Retrieved September 2009, from http://www.nielsen-online.com/pr/pr_090602.pdf

Ofcom (2008). Social Networking: A quantitative and qualitative research report into attitudes, behaviours and use. *Office of Communications Research Document*, April 2008.

Park, M. (2009, February 26). Legal issues to consider for Web 2.0. *Inspecht HR Futures Conference*, Melbourne, Australia. Retrieved September 2009, from http://www.slideshare.net/mspecht/legal-issues-to-consider-for-web-20

Parsons, K., McCormac, A., Butavicius, M. & Ferguson, L. (2010). Human Factors and Information Security: Individual, Culture and Security Environment. *DSTO Technical Report*, DSTO-TR2484.

Rosenblum, D. (2007). What anyone can know: The privacy risks of social networking sites. *IEEE Security and Privacy, 5(3)*, 40-49.

Ross, C., Orr, E.S., Sisic, M., Arseneault, J.M., Simmering, M.G. & Orr, R.R. (2009). Personality motivations associated with Facebook use. *Computers in Human Behavior, 25*, 578-586.

Schneier, B. (2009, August 11). The consequences of trusting our instincts. *The Age*. Retrieved October 2009, from http://www.theage.com.au/technology/the-consequences-of-trusting-our-instincts-20090811-efrb.html

Schwartz, J. (2005). High-Tech hot spots. *Newsweek, 146(8)*, 64-65.

Sherry, D. (2008). How to implement and enforce a social networking policy. *Mitigating Web 2.0 Threats, a Lesson in SesarchSecurity.com's Data Protection Security School*. Retrieved November 2009 from http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1338433_mem1,00.html

Skeels, M.M. & Grudin, J. (2009). When social networks cross boundaries: A case study of workplace use of Facebook and LinkedIn, *Proceedings of the 2009 International Conference on Supporting Group Work*, Sanibel Island, FL, USA: ACM Press, 95-104.

Sophos (2007, August 14). *Sophos Facebook ID Probe Shows 41% of Users Happy to Reveal all to Potential Identity Thieves*. Retrieved October 2009, from http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html

Steinfield, C., DiMicco, J.M., Ellison, N.B. & Lampe, C. (2009). Bowling online: Social networking and social capital within the organisation. *Proceedings of the Fourth International Conference on Communities and Technologies*, PA, USA: ACM Press, 245-254.

Strater, K. & Lipford, H.R. (2008). Strategies and struggles with privacy in an online social networking community. *Proceedings of the 22nd British HCI Group Annual Conference on HCI 2008: People*, Liverpool, UK: British Computer Society, 111-119.

Sutter, J. & Carroll, J. (2009, February 6). Fears of impostors increase on Facebook. *CNN*. Retrieved August 2009, from http://edition.cnn.com/2009/TECH/02/05/facebook.impostors/index.html

Tidwell, L. C., & Walther, J. B. (2002). Computer-mediated communication effects on disclosure, impressions, and interpersonal evaluations: Getting to know one another a bit at a time. *Human Communication Research, 28(3)*, 317–348.

Todd, M. A., DiJohn, J. L. & Aldridge, S. L. (2008) *Employee Use, Misuse, and Abuse of Social Network Sites*, Inquiry & Analysis, National School Boards Association, Alexandria, VA.

Twitter (2009). Twitter / Terms of Service. Retrieved November 2009 from http://twitter.com/tos

Wang, Y. & Kobsa, A. (2009). Privacy in online social networking at workplace, *Proceedings of the IEEE SocialCom'09 Workshop on Security and Privacy in Online Social Networking (SPOSN09)*, Vancouver, Canada.

Zhao, D. & Rosson, M.B. (2009). How and why people twitter: The role that micro-blogging plays in informal communication at work. *Proceedings of the 2009 International Conference on Supporting Group Work*, Sanibel Island, FL, USA: ACM Press, 243-253.

Zhao, D., Rosson, M.B. (2008). How might microblogs support collaborative work?, *Proceedings of CSCW 08 Workshop on Social Networking in Organizations*, November 9, San Diego, CA.

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION
DOCUMENT CONTROL DATA

1. PRIVACY MARKING/CAVEAT (OF DOCUMENT)

2. TITLE

Don't Judge a (Face)Book by its Cover: A Critical Review of the Implications of Social Networking Sites

3. SECURITY CLASSIFICATION (FOR UNCLASSIFIED REPORTS THAT ARE LIMITED RELEASE USE (L) NEXT TO DOCUMENT CLASSIFICATION)

Document	(U)
Title	(U)
Abstract	(U)

4. AUTHOR(S)

Kathryn Parsons, Agata McCormac and Marcus Butavicius

5. CORPORATE AUTHOR

DSTO Defence Science and Technology Organisation
PO Box 1500
Edinburgh South Australia 5111 Australia

6a. DSTO NUMBER	6b. AR NUMBER	6c. TYPE OF REPORT	7. DOCUMENT DATE
DSTO-TR-2549	AR-014-995	Technical Report	May 2011

8. FILE NUMBER	9. TASK NUMBER	10. TASK SPONSOR	11. NO. OF PAGES	12. NO. OF REFERENCES
2009/1170256/1	INT 07/012	ASINFOSEC	30	71

13. DOWNGRADING/DELIMITING INSTRUCTIONS

To be reviewed three years after date of publication

14. RELEASE AUTHORITY

Chief, Command, Control, Communications and Intelligence Division

15. SECONDARY RELEASE STATEMENT OF THIS DOCUMENT

Approved for public release

OVERSEAS ENQUIRIES OUTSIDE STATED LIMITATIONS SHOULD BE REFERRED THROUGH DOCUMENT EXCHANGE, PO BOX 1500, EDINBURGH, SA 5111

16. DELIBERATE ANNOUNCEMENT

No Limitations

17. CITATION IN OTHER DOCUMENTS Yes

18. DSTO RESEARCH LIBRARY THESAURUS http://web-vic.dsto.defence.gov.au/workareas/library/resources/dsto_thesaurus.shtml

Social Networking Sites, Human Factors, Information Security, Human Behaviour

19. ABSTRACT

Social networking sites (SNS) are increasingly popular, and as their popularity continues to grow, the integration of these sites within the workplace is vitally important. Although these sites may provide a number of advantages, such as improved knowledge sharing and improved relationships, there are also numerous risks associated with the use of these sites. For example, these sites may waste company time, may create tension within the workplace, and may jeopardise privacy, security and confidentiality. Hence, it is crucial for organisations to develop a clear and enforceable policy for the use of these sites, which should be coupled with a personal, meaningful and contextualised education campaign. It is vital to emphasise the possible risks, reinforce the restrictions to use, and stress the consequences of a failure to comply. This should help to ensure that organisations can benefit from the advantages of these sites, without unnecessarily jeopardising their security.